unless specifically authorized for such use. Flag personnel shall be furnished by the Contractor at points on apron and taxiway for safe guidance of its equipment over these areas to assure right of way to aircraft. Areas and routes used during the contract must be returned to their original condition by the Contractor. Airport management shall establish the maximum speed allowed at the airport. Vehicles shall be operated so as to be under safe control at all times, weather and traffic conditions considered. Vehicles must be equipped with head and taillights during the hours of darkness.

(End of clause)

3052.237–70 Qualifications of contractor employees.

As prescribed in (HSAR) 48 CFR 3037.110–70(a), insert the following clause:

QUALIFICATIONS OF CONTRACTOR EMPLOYEES (DEC 2003)

(a) ''Sensitive Information'' is any information or proprietary data which if subject to unauthorized access, modification, loss, or misuse could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. 552a (The Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(b) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(c) Contractor employees working on this contract must complete such forms, as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required.

(d) The Contracting Officer may require dismissal from work those employees deemed incompetent, careless, insubordinate, or otherwise objectionable, or whose continued employment is deemed contrary to the public interest or inconsistent with the best interest of national security.

(e) Each employee of the Contractor shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by an Alien Registration Receipt Card Form I–151. An alien authorized to work shall present evidence from the Bureau of Citizenship and Immigration Services that employment will not affect his or her immigration status.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

3052.237–71 Information technology systems access for contractors.

As prescribed in (HSAR) 48 CFR 3037.110–70(a) and (b), insert a clause substantially as follows. The contracting officer may specify additional IT security requirements unique to an OE.

INFORMATION TECHNOLOGY SYSTEMS ACCESS FOR CONTRACTORS (DEC 2003)

(a) No contractor personnel shall start work under this contract that involves actual or potential access to sensitive information until (1) approved for access, (2) they have received a security briefing, or current refresher, about Information Technology (IT) security, from the appropriate Organizational Element (OE) Information Systems Security Officer (ISSO); and (3) have signed a non-disclosure agreement form. This user security agreement is provided as an Attachment to this solicitation. By signing the user security agreement, the individual will be acknowledging their responsibility to properly use and safeguard all DHS OE information technology resources and information related thereto. The Contracting Officer Technical Representative (COTR) for this contract shall arrange the aforementioned security briefing. The ISSO is responsible for retaining the non-disclosure documents signed and submitted by the contractor employees as well evidence of security training.

(b) The contractor shall have access only to those areas of DHS OE information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Information technology assets includes computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and Internet sites. Any attempts by contractor personnel to gain access to any information technology resources not expressly